Network and Cyber Security Audit Hearing

Director Dave DeVries

House Committee on Oversight
April 12, 2017

DTMB

Audit Objective - Design and Administration of IT Network Configuration Management – Finding 1

Finding: Need to fully establish and implement configuration management controls

OAG Recommendation: Fully establish and implement effective configuration management controls for the State's network devices.

DTMB Response: Partially agrees with the recommendation. DTMB employs a defense-in-depth approach, including effective configuration management controls, that enable DTMB to protect the State's network from threats and vulnerabilities.

Updating internal standard for DTMB that adopts industry best practices used for secure configurations.

Remediation Status: Remediated 96% of the configuration exceptions to date. Revised policy to be completed in April 2018.

Remediation Method: IT Policy Review and Updates / Remediate Configuration Items

Audit Objective – Design and Administration of IT Network
Network Access Control– Finding 2

Finding: Network access control needed to help prevent unauthorized devices from connecting to the State's network

OAG Recommendation: Implement a NAC solution to help ensure that only authorized devices access the State's IT network and that unauthorized or unmanaged devices are detected and prevented from connecting.

DTMB Response: Partially agrees with recommendation. No single automated network access control (NAC) solution.

Conducting a limited pilot to determine the feasibility of implementing NAC.

Will control ports to disable those not actively used.

Remediation Status: Partially remediated / in-progress (10%)

Remediation Method: Controlling all switch ports/ Conduct NAC pilot

Audit Objective – Design and Administration of IT Network Network Device Update Management– Finding 3

Finding: Improved process needed for managing updates to network device operating systems

OAG Recommendation: Fully establish and implement an effective process for managing updates to the operating systems of network devices.

DTMB Response: DTMB agrees with this recommendation. Need to establish a formal written process for analyzing security vulnerabilities and updating network devices as necessary.

Remediation Status: Partially remediated / in-progress (60%); Completion in June 2018

Remediation Method: IT Policy Review and Updates

Audit Objective – Security and Access Controls
Firewall Controls – Finding 8

Finding: Controls over firewalls need to be improved to ensure security of the network.

OAG Recommendation: Establish and implement effective controls over the management of firewalls to help protect the State's network from threats.

DTMB Response: Agree with recommendation. Continue improvement of documentation, review, and approval of firewall rulesets in accordance with its effective controls in managing firewalls.

In February 2015, implemented a structured automated audit process to ensure firewall rules were implemented in compliance with State standards. DTMB continues to use this process for all new firewall rules and changes.

Old firewall methodology was to permit all, deny by exception. Since 2015, the methodology changed to "permit by exception."

Remediation Status: Partially Remediated/In Progress

Remediation Method: Move legacy to NGDI/Cloud First Strategy

Audit Objective – Monitoring of Network Security
Risk Management – Finding 11

Finding: Risk management practices not fully established and implemented

OAG Recommendation: DTMB fully establish and implement effective risk management practices over the State's IT network to help ensure that security risks are identified and sufficiently evaluated.

DTMB Response: Agree with recommendation.

Since October 2017, Implementing an effective risk management framework adopted from Federal agencies in accordance with NIST guidelines.

Part of Enterprise Risk Management Council. Risks Management signed by business owners and the State CIO indicate acceptance of the documented risk and mitigation measures.

Use a risk-based approach to evaluate improvements to the application/system test/validation.

Remediation Status: Partially Remediated/In Progress

Remediation Method: Security Accreditation Process

Audit Objective – Cyber Security Awareness Programs
Phishing – Finding 14

Finding: Continue cyber security awareness training program to help ensure that information system users maintain a secure environment and respond to cyber security threats appropriately.

OAG Recommendation: DTMB continue its cyber security awareness training program to help ensure that information system users maintain a secure environment and respond to cyber security threats appropriately.

We also recommend that DTMB take steps to ensure that all information system users participate in its cyber security awareness training program.

DTMB Response: Agree with this recommendation. DTMB continually improves its security awareness and training program. In August 2017, DTMB implemented Version 2.0 of its cyber security awareness training program. It includes a mechanism to assess the effectiveness of the program.

DTMB will continue to evaluate user participation in its security awareness program and begin to tie user's continued access to the network to their trends in participation in the program.

Reduced Administrative Users (elevated permissions) by 87%. Still reducing.

Remediation Status: Continuous improvement

Remediation Method: Cyber Security Training

Questions